CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

SJS CJCSI 3435.01
DISTRIBUTION: A, B, C, J, S 8 June 2004

Standards for Chemical, Biological, Radiological,
Nuclear, and High Yield explosive (CBRNE) PROTECTION
ON Installations AND FACILITIES

References: See Enclosure C

1. Purpose. This CJCSI provides interim standards for U.S. military installations and facilities for chemical, biological, radiological, nuclear, and high-yield explosives (CBRNE) protection. Installation protection is intended to serve as an enhancement to both planned and existing antiterrorism efforts as well as planned and existing incident management efforts. This CJCSI shall be incorporated into DODI 2000.16, DOD Antiterrorism Standards, *[See reference t]* during its next periodic update. The guidance contained herein shall remain in effect until CBRNE standards are fully integrated with DODI 2000.16. This Instruction:

a. Creates CBRNE standards for installation and facility protection, thereby ensuring U.S. warfighting capabilities worldwide. These standards align worldwide CBRNE protection initiatives with other incident management actions to prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies. CBRNE protection preserves military missions and personnel and is defensive in scope only. Antiterrorism (AT) includes defense of high-yield explosives (i.e., the "E" of CBRNE).

b. Implements reference (k), states policy, assigns responsibilities, and prescribes procedures under references (a) through (bb) to establish and implement Chairman of the Joint Chiefs Instructions (CJCSI) worldwide standards to help protect personnel on military installations or leased facilities from chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) incidents.

c. References (o), (t), and (w) providing guidance for protection of personnel and assets mostly from high-yield explosive (i.e., "E") incidents. The DOD antiterrorism (AT) program and unified facilities criteria (references aa and bb) provide criteria and construction standards to mitigate terrorist threats and installation vulnerabilities to terrorism. Reference (u) covers CBRNE protection guidelines for emergency responders. References (b) and (l) show how the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD-AT&L) has oversight of program planning, allocation, and use of resources for activities within the DOD for Installation and Facility CBRNE Protection. Reference (x) implements the DOD Critical Infrastructure Protection (CIP) Program.

(1) This document supplements incident management guidance to prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies and <u>does not</u> subsume references (o), (p), (q), (t), (u), (v), (w) or (x).

(2) For the purposes of this interim CJCSI, the explosive (i.e., "E") part of CBRNE refers to the high-yield explosives with a CBRN component only. See DODI 2000.16 for most high-yield explosive protection standards.

d. Dictates to commanders at all levels to add CBRN defense considerations to explosive threat preparations as they prepare to defend all installations. Commanders must also maintain the capability to detect, deter, mitigate, and recover from CBRNE incidents across the operational spectrum (e.g., following industrial accidents, at installation, in transit, on deployment, on maneuver, and during engagement). Initial response to all CBRNE incidents should consider terrorist involvement until ruled out by competent authority.

e. Directs commanders to orient defensive priorities to sense hazards, shape the situation, shield personnel, and implement appropriate installation CBRNE countermeasures in order to sustain critical operations.

f. Makes use of DOD's risk management framework that allows the Department to consider tradeoffs among fundamental objectives and fundamental resource constraints."

g. Does not constitute requirements that are fiscally unsupportable or constitute additional manpower requirements.

2. <u>Cancellation</u>. None.

3. <u>Applicability</u>. These standards govern the activities of the Joint Staff and its relationship with the Services in developing protection and CBRNE protection standards.

a. This Instruction applies to the Military Departments (i.e., "Services") and the Chairman of the Joint Chiefs of Staff (CJCS).

b. CJCS recommends other DOD entities, (i.e., Combatant Commands, DOD Agencies, DOD Field Activities, the Office of the Secretary of Defense, the Office of the Inspector General of the Department of Defense) elect to follow this guidance as well since it is DOD policy "to protect personnel on military installations and DOD-owned or leased facilities from CBRNE attacks…." *[See references (k) and (m)]* Further, the intent is to incorporate this information into DODI 2000.16, Antiterrorism Standards, which will make it applicable for all of DOD. *[See reference (t)]*

c. The term "Services" refers to the Army, Navy, Air Force, Marine Corps, and Coast Guard *[reference (a)].* Note: Coast Guard efforts are funded through Department of Homeland Security and coordinated with DOD.

d. This Instruction is applicable in both CONUS and OCONUS.

e. This Instruction is applicable to all installations as well as autonomous facilities (i.e., DOD-owned or leased). Facilities, to include tenants, located on or grouped with an installation will develop supporting synchronized CBRNE protection procedures.

(1) In this Instruction, the term "installation" is meant to include designated "DOD-owned or leased facilities" as well.

(2) Questions regarding facilities having its own program should be referred to the owning COCOM, owning Agency, or J-8 Joint Requirements Office for Chemical, Biological, Radiological, and Nuclear (JRO-CBRN) Defense.

(3) Note: Analysis using Critical Infrastructure Protection methodology may help identify facilities to protect within installations.

4. Policy. In accordance with references (k) and (m), it is DOD policy:

a. To protect personnel on military installations and DOD-owned or leased facilities from CBRNE incidents, to respond to these incidents with trained and equipped emergency responders, and to ensure installations are able to continue critical operations during an incident and to expeditiously resume essential operations after an incident.

(1) CBRNE attacks may be focused on the following:

(a) Vulnerabilities of our national infrastructure outside the U.S. upon which the DOD must depend to execute the National

Military Strategy (NMS).

(b) Difficulties in effectively safeguarding personnel working or living on DOD installations and facilities from CBRNE effects.

(2) Many of our past efforts have focused on enhancing protection and response capabilities to high-yield explosive (i.e., "E") and other terrorist methods, but DOD must address potential CBRN threats as well.

b. To develop a DOD-wide concept of operations for the defense of military installations and DOD-owned or leased facilities against CBRNE incidents. The concept of operations must address how to deter CBRNE incidents, and if deterrence is not successful, to detect, warn and protect personnel from such incidents, and respond appropriately to mitigate the impact of incidents. This concept should address the continuity of critical military missions and the prompt restoration of essential installation operations should those operations be interrupted. In CONUS and OCONUS, plans and preparations shall be done in conjunction with local/host nation authorities through mutual aid agreements, memorandums, host nation agreements, etc., (where possible) to protect personnel and assure critical infrastructure.

c. To establish primary CBRNE protection standards by integrating CBRN defense and terrorist defense (i.e., high-yield explosives) efforts. To ensure integrated CBRNE standards are developed, the Force Protection Functional Capabilities Board (FCB) will provide initial oversight. Within CBRNE protection, J-8 JRO-CBRN Defense will provide functional expertise for CBRN defense and J-34 will provide functional expertise regarding high-yield explosives (i.e., "E").

d. To provide appropriate levels of CBRNE protection for personnel at installations and facilities, based on appropriate procedures, equipment and training. This includes military personnel, DOD civilians, other persons who work on the installations and facilities, and family members assigned overseas or who work or live on our installations and facilities worldwide. Protection will be determined by a thorough assessment of the threat, vulnerability, criticality and risk associated with each installation.

(1) Emergency responders. Personnel who work closest to known or suspected CBRNE hazards (e.g., emergency responders) should be given the highest level of protection. In today's uncertain environment, responders should use maximum possible protection until determined otherwise by competent authority.

(2) Critical Personnel. Personnel deemed essential to the performance of critical military missions (whether military, civilian, contractor, host nation

personnel or third country nationals) should be provided an appropriate level of protection to support continuity of those critical military missions. Since critical missions should be continued without interruption, collective or individual protection may be necessary to sustain critical missions.

(3) Essential Personnel. Personnel deemed essential to the performance of essential military operations (whether military, civilian, contractor, host nation personnel or third country nationals) should be provided an appropriate level of protection to support near continuity for those essential military operations. Since essential operations may be interrupted for relatively short periods (i.e., hours to days), escape protection may be necessary to sustain essential operations (i.e., escape, survive, and restore essential operations).

(4) Other People. For all other persons not in the above categories, the objective will be to provide the procedures or protection necessary to safely survive an incident. Evacuation procedures, for example, may fulfill this requirement.

e. That Commanders at all levels are responsible for protecting persons and property subject to their control and have the authority to enforce CBRNE protection efforts. Nothing in this Instruction will detract from, or conflict with, the inherent and specified authorities and responsibilities of Commanders.

5. Definitions. Refer to Glossary Part II.

6. Responsibilities. The Chairman of the Joint Chiefs of Staff shall:

a. Prepare joint doctrine, develop assessment schedules, and assist the Assistant to the Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs [ATSD (NCB)] to develop and maintain DOD CBRNE protection standards in accordance with DODD 2000.12 *[See reference (o)].*

b. Ensure appropriate installation worldwide threat estimates are established in cooperation with Defense Intelligence Agency and U.S. Department of Homeland Security (as appropriate for CONUS and OCONUS). These threat estimates will be properly disseminated, shared, and used as the basis for capability definitions and support for DOD CBRNE protection efforts.

c. Direct the Joint Requirements Oversight Council to address DOD CBRNE protection issues.

d. Ensure the Chairman's Program Review and the Chairman's Program Assessment includes a summary of DOD CBRNE protection requirements as determined by the Joint Requirements Oversight Council and derived from the Combatant Commander's Integrated Priority Lists.

e. Place, as appropriate, priority on institutionalized training, exercises, leader awareness, and planning to support DOD CBRNE protection.

f. Address DOD CBRNE protection considerations in coordination with the Components.

g. Direct the J-8 Joint Requirements Office for CBRN Defense (JRO-CBRN Defense) to:

(1) Serve as the Joint Staff lead office for all CBRN Defense issues.

(2) Coordinate this CJCSI with the Joint Program Executive Office for Chemical-Biological Defense (JPEO-CBD).

(3) Develop a DOD CBRNE Protection Modernization Plan and update annually.

(4) Assist the Components to implement and standardize DOD CBRNE Protection.

(5) Integrate these standards with DODI 2000.16 *[See reference (t)]* and provide updates to pertinent guidance as CBRNE protection integration matures.

(6) Develop DOD-wide Concepts of Operation with corresponding requirements for personnel, equipment, and training.

7. Summary of Changes. Not applicable (new Instruction).

8. Releasability. This Instruction is releasable via the Internet Joint Electronic Library site, but only to .mil and .gov users. U.S. Military and other Federal government agencies may obtain copies of this CJCSI through the Internet on the CJCS Directives Home Page -- http://www.dtic.mil/doctrine/jel/cjcsd.htm. If authorized, copies are also available through the Government Printing Office on the Joint Electronic Library CD-ROM.

9. Effective Date. This Instruction is effective upon receipt and remains in effect until CJCS or DJS rescinds.

Director, Joint Staff

(INTENTIONALLY BLANK)

DISTRIBUTION

Distribution A, B, C, and J plus the following:

	Copies
Secretary of Defense	4

(INTENTIONALLY BLANK)

LIST OF EFFECTIVE PAGES

The following is a list of effective pages for this Instruction. Use this list to verity the Instruction's currency and completeness. An "O" indicates a page in the original publication.

PAGE	CHANGE	PAGE	CHANGE
1 thru 6	O	B-1 thru B-8	O
i thru viii	O	C-1 thru C-2	O
A-1 thru A-8	O	GL-1 thru GL-14	O
A-A-1 thru A-A-4	O		

(INTENTIONALLY BLANK)

RECORD OF CHANGES

Change No.	Date of Change	Date Entered	Name of Person Entering Change

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

ENCLOSURE A

CJCS CBRNE PROTECTION STANDARDS

1. CJCS STANDARD 1: Implement CJCS CBRNE Protection Policy. The Military Departments (i.e., "Services") and the Chairman of the Joint Chiefs of Staff (hereafter referred to collectively as the "Components") are responsible to implement CBRNE protection policies within their organizations. Components shall:

a. Coordinate with the Joint Requirements Office for CBRN Defense (J-8 JRO-CBRN Defense) to implement and standardize CBRNE protection across the Components.

b. Coordinate with the J-8 JRO-CBRN Defense to determine a methodology to establish baseline capabilities and standards needed to implement appropriate CBRNE protection actions. These actions shall protect personnel and identify CBRNE-specific vulnerabilities in coordination with incident management needs to prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies.

c. Develop and implement CBRNE protection capabilities at installations and DOD-owned or leased facilities and comply with the standards contained in this Instruction.

2. CJCS STANDARD 2: Supplements to CBRNE Protection Standards. As a minimum, Components shall supplement the CBRNE protection standards to:

a. Address procedures to collect and analyze CBRNE threat information, threat capabilities, and vulnerabilities to CBRNE incidents.

b. Include CBRNE threat assessment, vulnerability assessments, and CBRNE incident response (including incident management).

c. State how installations shall develop, train, exercise, maintain, sustain, and assess integrated installation preparations to protect military installations from CBRNE incidents, to respond to CBRNE incidents with trained and equipped emergency responders, to ensure installations are able to continue critical missions during an incident, and to resume essential operations after an incident. These efforts shall be done in coordination with the incident management activities to prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies) in order to encourage cross-functional cooperation and minimize potential redundancies.

3. CJCS STANDARD 3: CBRNE Protection, Response Capabilities, and Prioritization Criteria. Component and agency leaders shall establish CBRNE

Protection and Response capabilities at all appropriate installations. These capabilities should be organic but may be supported by local/host-nation agencies through appropriate agreements.

a. DOD installations designated by the appropriate Components are responsible to establish CBRNE protection capabilities.

b. Components shall develop a methodology that allows them to identify and prioritize DOD missions for which they are responsible to justify enhancements (i.e., to include CBRNE protection). Components shall prioritize critical mission and infrastructure nodes that can affect an installation's (or tenant's) ability to perform its respective DOD missions. This is a joint responsibility of the Components and the agencies.

c. Regardless of the provision of the installation CBRNE protection capabilities, all installation equipment, training and CONOPS will be standardized to ensure interoperability of response and support forces using CJCS- and service-identified equipment lists and training.

4. CJCS STANDARD 4: Management and Oversight of CBRNE Protection and Response. Commanders at all levels shall develop and implement comprehensive CBRNE protection and response capabilities for installations under their respective control. The standards contained in this Instruction are designed to reduce an installation's vulnerability to accidental or intentional release of CBRNE contamination.

a. CBRNE Management. Components shall consider establishing a full-time CBRNE Protection Officer and staff. Components shall assign in writing sufficient CBRNE Protection Officers for each appropriate installation.

b. Comprehensive CBRNE protection oversight includes risk management (which includes threat, criticality, vulnerability, and risk assessments), planning, training and exercises, resource generation, and program reviews. The process, or sequence, of CBRNE protection elements should be iterative and serve continuously to refine and improve CBRNE protection capabilities.

c. Close coordination between incident management actions to prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies shall significantly assist planning, execution, and recovery.

d. The appropriate COCOM with geographic responsibility shall make decisions for installations under their purview when CBRNE protection responsibilities conflict, overlap, or are not otherwise governed by law, a specific DOD policy, or an appropriate memorandum of agreement. That COCOM will then refer the issue to the J-8 JRO-CBRN Defense for resolution.

5. CJCS STANDARD 5: CBRNE Protection Coordination. Combatant Commanders (COCOMs) with geographic responsibilities should prepare actions or action plans to address CBRNE incidents on DOD installations in their respective areas of responsibility and update annually. The CBRNE plan may be integrated with the Antiterrorism Plan.

a. Assistant Secretary of Defense for Homeland Defense (ASD(HD)) is the lead DOD focal point for Department of Homeland Security (DHS) interface regarding coordination with the designated Lead Federal Agencies. Coordination with host nation authorities or Chiefs of Mission will be in accordance with appropriate Geographic COCOM guidance.

b. COCOMs should be familiar with local, state, or regional plans as well as any Status of Forces Agreements (SOFAs) and other international agreements affecting CBRNE incident response as well as host-nation capabilities (or U.S. Chiefs of Missions) to assist.

c. Installation commanders shall plan, prepare, and conduct integrated CBRNE protection exercises annually in conjunction with local authorities. Integrated CBRNE protection exercises may be conducted in conjunction with antiterrorism exercises.

6. CJCS STANDARD 6: Threat Information Collection and Analysis. Commanders will develop a system to gather, analyze, and disseminate threat information (including CBRNE incident threats) in accordance with DODI 2000.16 *[See reference (t)].*

7. CJCS STANDARD 7: Threat Information Flow. Commanders shall disseminate all CBRNE threat information (subject to release limitations) in accordance with DODI 2000.16 *[See reference (t)].*

8. CJCS STANDARD 8: Installation CBRNE Protection Risk Assessments. Components shall prepare Installation CBRNE Protection Risk Assessments at least annually for designated installations. Commanders shall do Installation CBRNE Protection risk assessments concurrent with other related risk assessments (i.e., incident management actions to prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies). These assessments will be a factor in justifying CBRNE protection enhancements, risk management, program/budget requests, and applying CBRNE protection actions. Risk assessments will analyze the following elements:

a. Installation threats *[See CJCS Standard 6].*

b. Criticality of installation missions.

c. Vulnerability to installation threats. *[See CJCS STANDARD 9]*

d. The ability to conduct activities to deter CBRNE incidents, employ countermeasures, mitigate the effects of a CBRNE incident, and recover from a CBRNE incident. *[Note: Emergency response is covered under reference (u).]*

9. CJCS STANDARD 9: Installation CBRNE Protection Vulnerability Assessment**.** Installation commanders shall ensure all related Vulnerability Assessments (e.g., incident management actions to prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies) are coordinated with other assessing entities and to the degree possible integrated and conducted in accordance with DODI 2000.16 *[See reference (t)].* These assessments will include CBRNE threats posed by nearby commercial activities (e.g., chemical plants) and transportation modes (e.g., truck and rail). Subject matter experts from the related vulnerability assessments (i.e., incident management) should supplement AT subject matter experts when completing Installation CBRNE Protection Vulnerability Assessments.

10. CJCS STANDARD 10: CBRNE Protection Planning. Installation commanders shall ensure comprehensive CBRNE protection planning is included in their AT Plan in accordance with DODI 2000.16 *[See reference (t)].* Installation Incident Response defensive actions will be in accordance with DODI 2000.18 *[See reference (u)].* CBRNE protection planning shall include considerations for protecting tenant commands that rely on a common emergency response capability and require coordinated mass notification, evacuation, sheltering, and casualty care plans. Installation commanders shall also consider including nearby commercial CBRNE activities in their planning.

11. CJCS STANDARD 11: CBRNE Personnel Protection on Installations. Commanders shall reduce vulnerability to CBRNE incidents and begin to provide CBRNE protection for persons who work or live on DOD installations. Components should coordinate with the J-8 JRO-CBRN Defense regarding protection, which shall be based on appropriate policies, procedures, equipment training, and Service resourcing. *[See references (k) and (u)]* Priority to reduce personnel protection vulnerabilities (in order of importance) shall be to protect emergency responders who potentially face the highest CBRNE challenge levels, personnel needed to continue critical missions, personnel needed to accomplish essential operations, and all other personnel.

a. Emergency responders. Personnel who work closest to known or suspected CBRNE hazards (e.g., emergency responders) should be given the highest level of protection. In today's uncertain environment, responders

should use maximum possible protection until determined otherwise by competent authority.

b. Critical Personnel. Personnel deemed essential to the performance of critical military missions (whether military, civilian, contractor, host nation personnel or third country nationals) should be provided an appropriate level of protection to support continuity of those critical military missions. Since critical missions should be continued without interruption, collective or individual protection may be necessary to sustain critical missions.

c. Essential Personnel. Personnel deemed essential to the performance of essential military operations (whether military, civilian, contractor, host nation personnel or third country nationals) should be provided an appropriate level of protection to support near continuity for those essential military operations. Since essential operations may be interrupted for relatively short periods (i.e., hours to days), escape protection may be necessary to sustain essential operations (i.e., escape, survive, and restore essential operations).

d. All Other Personnel. For all other persons not in the above categories, the objective will be to provide the procedures or protection necessary to safely survive an incident. Evacuation procedures, for example, may fulfill this requirement.

e. Included as part of the above categories are:

(1) Those who work or live on DOD installations worldwide.

(2) Family members authorized overseas.

(3) Contractors if designated in contract agreements and designated as essential to perform critical DOD missions *[See CJCS Standard 11a, above]*.

12. CJCS STANDARD 12: CBRNE Incident Response Actions. Installation commanders shall prepare incident emergency response actions in accordance with DODI 2000.18 *[See reference (u)]*.

13. CJCS STANDARD 13: CBRNE Incident Management Actions. Installation commanders shall prepare integrated CBRNE incident management actions to supplement installation AT incident response actions, allowing response and recovery actions to continue. Installation commanders shall:

a. Where multiple installations rely on common infrastructure or emergency response assets, intraservice and interservice support agreements shall be developed to ensure the most effective use and protection of common assets.

b. Develop and review annually mutual aid agreements, host nation agreements, etc., as required with local emergency responders, outlining cooperative defensive actions where the military can assist civilian emergency response (and vice versa) during response to CBRNE incidents.

(1) Mutual aid agreements (etc.) shall address specific capabilities under law enforcement, firefighting, medical surveillance, medical treatment, hazardous materials response, explosive ordnance disposal, public health, and CBRNE incident management.

(2) When applicable, mutual aid agreements must address CBRNE mass casualties.

(3) An installation's Battle Staff (or designated alternate) shall handle requests for assistance from state and local officials when mutual aid-type agreements do not exist.

c. Coordinate annually with civilian community (i.e., counterpart) emergency operations centers to identify and update responsible points of contact, emergency protocols, and expectations in the event of a CBRNE incident on or near the installation.

d. Consider designating a Joint Information Center to handle media demands and information control in the event of a CBRNE incident on or near the installation.

(1) Ensure policies and procedures are consistent with the US Government's "No Double Standard" policy and that procedures have been coordinated in advance with higher headquarters and any federal, local, state, U.S. mission, and host government staff elements that may be involved in its execution.

(2) If the incident is declared to be a "terrorist act," then responsibility for resolving the situation may pass to another agency. If so, the gaining agency assumes the lead for public affairs activities and the military PAO will act in a support role.

e. Coordinate annually with civilian emergency response counterpart information/public affairs centers to identify and update responsible points of contact, emergency protocols, and media expectations.

f. Be knowledgeable about the Federal Response Plan – Interim, the Initial National Response Plan, and the National Incident Management System (NIMS) *[See references (c), (e) and (f)]*. Be prepared to coordinate and support the lead federal agencies in the event of a CBRNE incident.

g. Determine the extent of CBRNE hazards on that installation, as consistent with the CBRNE protection equipment available.

h. Procedures exist to collect samples IAW established sampling protocols.

i. Be capable of rapid notification of all appropriate personnel on an installation of CBRNE hazards. *Note: Outside CONUS, this includes sponsored dependents living off-site.*

j. Be capable of activating appropriate medical responses (e.g., prophylaxis, vaccines, diagnosis, treatment, etc.) to a CBRNE terrorist incident

k. When available, protect civilians using civilian-approved equipment (e.g., Occupational Safety and Health Administration and National Institute for Occupational Safety and Health standards). *[See reference (u) for emergency responder requirements.]* OCONUS, in the case of contractors and local national civilians, equipment satisfying host nation standards may be substituted. Services will program to satisfy these requirements.

14. CJCS STANDARD 14: CBRNE Protection Sustainment and Recovery Actions. Installation commanders shall prepare defensive actions to sustain critical missions and recover essential operations following a CBRNE incident. Commanders must identify sites where mitigation might nullify or degrade the effectiveness of a CBRNE incident as well as the most critical missions and facilities to recover first should an incident occur. Defensive actions to sustain critical missions and recover essential operations should reduce potential degradation caused by a terrorist attack. Critical missions must be sustained and recovery of essential military operations should be swift.

15. CJCS STANDARD 15: Comprehensive CBRNE Protection Review. Installation Commanders shall comprehensively review their CBRNE protection capabilities, as integrated in their AT program and plans, at least annually to facilitate CBRNE protection capability enhancements. Services will ensure subordinate installation capabilities and plans are reviewed by a higher headquarters on an annual basis.

16. CJCS STANDARD 16: Training and Exercises. Installation commanders shall conduct regular field and staff training, as well as exercise integrated AT and CBRNE protection plans at least annually. CBRNE protection training and exercises will be done in conjunction with DODI 2000.16 *[reference (t)]* and should include (as appropriate) local, state, regional, federal, and/or host nation agencies. CBRNE protection training and exercises shall be integrated into AT training and exercises, plus CBRNE protection shortfalls shall be identified at the same time as AT shortfalls. To incorporate lessons learned, commanders should maintain exercise documentation for at least three years.

17. CJCS STANDARD 17: General Requirements for CBRNE Protection Training. Components shall ensure all assigned personnel receive appropriate training to advance CBRNE protection awareness.

a. Antiterrorism training *[See DODI 2000.16, reference (t)]* shall contain integrated CBRNE protection training.

b. Emergency Responder Training. See DODI 2000.18. *[See reference (u)]*

18. CJCS STANDARD 18: Construction Considerations. Components shall adopt and adhere to common criteria and minimum construction (i.e., new construction, renovation, or rehabilitation) standards to mitigate CBRNE protection vulnerabilities and threats. *[See references (o), (t), (w), (aa), and (bb).]*

19. CJCS STANDARD 19: Components shall use DOD AT Minimum Construction Standards for Buildings *[See reference (aa)]*, specifically those standards that address CBRNE protection. The Site Selection Criteria will determine if potential DOD installations, either currently occupied or under consideration for occupancy by DOD personnel, can adequately protect occupants against a CBRNE incident. Circumstances may require the movement of DOD personnel or assets to facilities the U.S. Government has not previously used or surveyed.

20. CJCS STANDARD 20: CBRNE Protection Considerations for Mail. Components shall adopt and adhere to postal criteria and standards to mitigate CBRNE protection vulnerabilities and threats. See reference (aa) for construction standards for mail facilities.

21. CJCS STANDARD 21: "Sense." Installations shall be able to "Sense" CBRNE Incidents.

a. Develop, maintain, and execute CBRNE protection tactics, techniques, and procedures to include "sense" operational concepts.

b. Realize a CBRNE incident occurred.

c. Determine immediate CBRNE hazards and define hazard locations.

d. Identify (as appropriate) the CBRNE hazards involved.

e. Plan installation sensor locations, testing procedures, and C4I to support those testing locations.

f. Be prepared to preserve CBRNE evidence, collect CBRNE samples in accordance with established sampling protocols for CBRNE incidents,

and implement appropriate CBRNE chain of custody rules.

22. CJCS STANDARD 22: "Shape." Installations shall:

a. Develop, maintain, and execute CBRNE protection tactics, techniques, and procedures to include "shape" operational concepts.

b. Develop and maintain CBRNE protection emergency response guidelines IAW DODI 2000.18.

c. Distinguish critical, essential, and other missions and operations to support "Sense," "Shield," and "Sustain" determinations.

d. Assess CBRNE incidents as they develop and notify local, state, federal, host nation and Service emergency response agencies as appropriate.

e. Be prepared to transition installation CBRNE incidents to federal control and then back to DOD control for long-term restoration and recovery.

f. Identify potential temporary disposal sites for hazardous waste generated by a potential CBRNE incident, as appropriate.

23. CJCS STANDARD 23: "Shield." Installations shall:

a. Develop, maintain, and execute CBRNE protection tactics, techniques, and procedures to include "shield" operational concepts.

b. Protect personnel as appropriate for a CBRNE incident and depending on DOD mission criticality.

c. Plan medical countermeasures for CBRNE incidents.

d. Be prepared to handle contaminated casualties (psychological, injured, or fatalities) both at the incident site and at military medical facilities.

e. Suppress residual CBRNE hazards while protecting evidence.

24. CJCS STANDARD 24: "Sustain." Installations shall:

a. Develop, maintain, and execute CBRNE protection tactics, techniques, and procedures to include "sustain" operational concepts.

b. Continue critical missions despite CBRNE incidents, if possible.

c. Restore essential operations quickly following CBRNE incidents.

25. CJCS Standard 25: CBRNE Resource Requirements. Commanders shall identify CBRNE resource requirements using the DoD Planning, Programming, Budgeting and Execution (PPBE) process. Emergent/Emergency and unfunded CBRNE requirements must be submitted through the appropriate COCOM in accordance with DoDI 2000.16."

(INTENTIONALLY BLANK)

APPENDIX A TO ENCLOSURE A

CBRNE Protection Metrics		
Standard #	**CJCS Installation Standard**	**Metric**
1.a.	Components review and update CBRNE protection and response capabilities with JRO-CBRN Defense	Annually
1.b.	Components determine baseline capabilities and standards	Annually
2.	Components review their supplement to CBRNE protection standards for adequacy	Annually
2.a	Components review CBRNE threats and vulnerabilities with Intelligence community	Annually
2.c	With Service support, installation commanders shall equip, train, and exercise personnel appropriately to accomplish integrated installation CBRNE protection	Annually
3	Installation CBRNE protection and response capabilities reviewed for adequacy (includes mutual support memorandums, as appropriate)	Annually
3.b	Component and agency leaders shall identify critical DOD missions and infrastructure nodes on installations and facilities	Annually
4.a	Installations consider assigning CBRNE Protection Officer	Annually
5.	Combatant Commanders with geographic responsibilities shall prepare action plans to address CBRNE incidents in their respective areas of responsibility and update annually	Annually
5.c.	Installations will conduct integrated AT CBRNE protection emergency response exercises in conjunction with local authorities	Annually
6.	CBRNE Threat information collected IAW DODI 2000.16	Continuously
7.	CBRNE threat information flow procedures are IAW DODI 2000.16	Annually
8.	Components complete Installation CBRNE Protection Risk Assessments	Annually

9.	Vulnerability assessment completed IAW DODI 2000.16 integrating incident management to prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies.	Annually
9	Incident management subject matter experts (i.e., SMEs who prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies) shall supplement AT personnel to assess Installation Vulnerability	Annually
10	Comprehensive CBRNE protection planning is included in the installation AT plan IAW DODI 2000.16	Annually
10	Comprehensive installation incident response is included in the installation AT plan IAW DODI 2000.18	Annually
11	CBRNE protection includes planning for appropriate levels of CBRNE protection for persons who work or live on DOD installations	Annually
11.a.	Personnel deemed essential to perform critical DOD missions (i.e., military, civilian, contractor, host nation, or third-country nationals) are identified, trained, and provided an appropriate level of protection to support mission continuity	Identified, trained, and equipped
11.b	Protection or procedures are in place for others to survive a CBRNE incident (e.g., those who live or work on DOD installations worldwide, family members authorized overseas, and contractors if designated in contract agreements and designated as essential to perform critical DOD missions)	Identified, trained, and equipped as appropriate
12.	Incident response actions are IAW DODI 2000.18	Annual
13	Integrated CBRNE incident management actions are in place	Annual
13.a(1)	Appropriate mutual aid defensive agreements (host nation agreements, etc.) for emergency response are signed	Annual
13.a(2)	Mass CBRNE casualty procedures exist	Annual
13.b.	Points of contact for civilian counterpart functions are available in each control center	Annually

13.c.	Media center considered to handle CBRNE incident information control	Annually
13.d	Public affairs centers have identified points of contact, emergency protocols, and media expectations	Annually
13.e.	Procedures to coordinate and support lead federal agencies following a CBRNE incident are available	Annually
13.f.	Procedures exist to determine the extent of CBRNE hazards, as consistent with the CBRNE protection equipment available	Annually
13.g	Procedures exist to collect samples IAW established sampling protocols	Annual
13.h.	Be capable of rapidly notifying all appropriate personnel on an installation of CBRNE hazards *[Note: Outside CONUS, this includes sponsored dependents living off-site.]*	5 minutes
13.i.	Be capable of activating appropriate medical responses (e.g., prophylaxis, vaccines, diagnosis, treatment, etc.) to a CBRNE terrorist incident	15 minutes
13.k	When available, protect civilians using civilian-approved equipment (e.g., OSHA and NIOSH standards). OCONUS, in the case of contractors and local national civilians, equipment satisfying host nation standards may be substituted.	Annually
14.	Action plans are in place to sustain critical mission operations	Yes
14.	Action plans are in place to recover essential operations from a CBRNE incident	Yes
15.	CBRNE protection and response capabilities reviewed comprehensively	Annually
16.	CBRNE protection and response plan exercised	Annually
16.	Exercise lessons learned - document and retain	Annually
17.a	AT training contains integrated CBRNE protection training. AT training is provided and documented IAW DODI 2000.16	Annually
17.b.	Emergency Responder training provided and documented IAW DODI 2000.18	Annually
18.	Installations use appropriate CBRNE protection construction standards	Yes

19.	Site selection criteria has been modified to include CBRNE protection concerns	Yes
20.	Procedures for mail handling include CBRNE protection concerns	Yes
21.a	Tactics, techniques, and procedures exist to "sense" CBRNE incidents	Annually
21.f	Be prepared to preserve CBRNE evidence, collect samples, and implement sample chain of custody rules.	Annually
22.a	Tactics, techniques, and procedures exist to "shape" CBRNE incidents	Annually
22.b	Procedures for CBRNE emergency response are IAW DODI 2000.18	Annually
22.c	Distinguish critical, essential, and other missions on the installation	Annually
22.e	Procedures to transition installation CBRNE incident control to federal control and then back to DOD for long-term restoration and recovery	Annually
22.f	Identify potential disposal sites for hazardous waste generated by a potential CBRNE incident	Annually
23.a	Tactics, techniques, and procedures exist to include "shield" operational concepts	Annually
23.b	Procedures exist to protect installation personnel from a CBRNE incident depending on mission criticality	Annually
23.c	Procedures exist for medical countermeasures for CBRNE incidents	Annually
23.d	Procedures exist to handle contaminated casualties (psychological, injured, or fatalities) at a CBRNE incident site and at military medical facilities	Annually
23.e	Procedures exist to suppress residual CBRNE hazards while protecting evidence	Annually
24.a	Tactics, techniques, and procedures exist to include "sustain" operational concepts	Annually

Table A-A-1. CBRNE Protection Metrics

ENCLOSURE B

How Related Programs Interact

1. The Joint Staff's Force Protection Functional Capabilities Board (FCB) is developing a Protection Functional Concept for the joint force. Protection requirements shall include personnel and infrastructure protection (including explosive [E] protection), countering weapons of mass destruction (WMD) operations (including CBRN defense), and other areas.

2. The DOD AT Program *[See reference (o)]*:

   a. Guidance and measures address terrorist use of high-yield explosives (E) (i.e., the "conventional" terrorist threat). Protection concepts against CBRN terrorist threats, though, currently are not well integrated into CBRNE incident response (especially in CONUS). These standards help integrate CBRN defense into the existing AT framework.

   b. Stresses preventive measures including threat analysis, installation criticality and vulnerability assessments, threat assessment, personal security, physical security, incident management, training, exercising, and public affairs. These initiatives are also applicable to CBRN terrorist incidents.

Combating Terrorism (CbT)	Definitions	CBRNE Protection Integration Requirements
Counterterrorism	Offensive measures taken to prevent (preempt), deter (disrupt), and respond to terrorism	Response expanded to include and integrate CBRNE hazards
Antiterrorism	Defensive measures used to reduce the vulnerability of individuals and property	WMD defense expanded to integrate CBRNE protection needs toward installation protection.
Intelligence Support	Information and knowledge about an adversary	Expand knowledge base to better address integrated CBRNE protection needs
Consequence Management	Measures taken to protect public health and safety, restore essential services, and provide emergency relief	Plan applicable Federal, state, local, and host nation emergency response to include CBRNE incidents

Table B-1. CBRN Defense Integration into DOD AT Efforts

c. Must integrate with CBRN to create comprehensive CBRNE protection *[See reference (m)].* How CBRN defense integrates into DOD antiterrorism is illustrated in Table B-1.

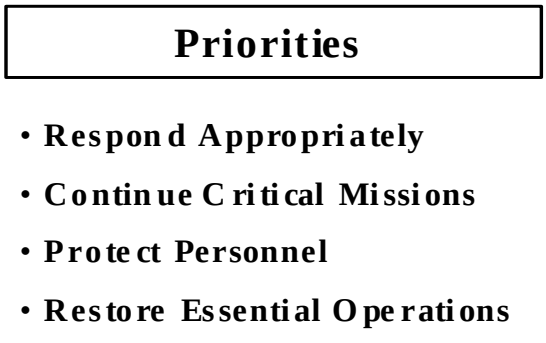

Figure B-1. Department of Defense Priorities

3. Department of Defense Priorities. Important to note are the DOD overarching philosophies to respond appropriately, continue critical missions, protect personnel, and restore essential operations.

a. Respond Appropriately. Respond appropriately with emergency responders to mitigate the impact of CBRNE incidents. As personnel closest to CBRNE hazards, emergency responders receive the highest level of protection. CBRNE incident response must balance the needs to assess the situation, secure the area, find and suppress hazards (e.g., fires, UXOs, contamination), establish control, evacuate personnel as appropriate, and handle casualties while preserving evidence.

(1) Ensure plans exist to establish immediate CBRNE hazard areas and predict downwind hazard areas.

(2) Ensure the installation can warn the population in the hazard area within 10 minutes of a known, reported CBRNE incident.

(3) Ensure the installation can evacuate the population in the hazard area within 15 minutes of a known, reported CBRNE incident.

b. Continue Critical Missions. Any mission deemed critical to the successful completion of DOD operations in peace, crisis and war (as outlined in the National Military Strategy) must continue operating and be protected from disruption, degradation, and destruction plus be restored quickly if damaged. Facilities, equipment, and personnel critical

to continue critical missions shall receive highest priority for protection.

c. Protect Personnel. Evacuate or protect personnel (as appropriate) in the hazard area (including downwind) that are not involved in CBRNE incident response or continuing critical missions.

(1) The highest level of protection is usually required for those who are closest to the CBRNE hazard (e.g., emergency responders).

(2) Personnel deemed essential to perform critical military missions (whether military, civilian, contractor, host nation personnel or third country nationals) should have an appropriate level of protection to support critical mission continuity for at least 12 hours.

(3) Equip the installation emergency responders with the appropriate capabilities to operate in a CBRNE hazard environment while responding to a CBRNE incident. These capabilities must be interoperable and to the same standard as civilian emergency responders.

(4) For all other personnel, installations shall provide procedures or protection necessary to safely survive an incident.

(a) Evacuation may be the best action to protect most personnel from the effects of a CBRNE incident. Evacuation or shelter-in-place procedures are usually preferred over issuing protective masks and suits.

(b) At least 90 percent of the hazard areas on an installation must be evacuated or protected (individual, collective, or sheltered-in-place) within 20 minutes of CBRNE contamination release.

d. Restore Essential Functions. Operations deemed less than critical but still essential to the successful completion of DOD critical missions in peace, crisis, and war. Essential functions must be reasonably protected from disruption, degradation, and destruction plus be restored quickly if damaged. Facilities, equipment, and personnel necessary to continue essential functions shall receive the next highest priority for protection.

4. The CBRN Defense Joint Enabling Concepts (See Figure B-2). Originally developed to support warfighters, an overview of CBRN Defense Joint Enabling Concepts is shown in Figure B-2 (above). The Joint Staff is institutionalizing integrated installation/facility CBRNE protection, starting with integration into antiterrorism (AT). Sense, shape, shield, and sustain (i.e., the 4 S's) describe the fundamental concepts within Installation CBRN Defense merging with AT.

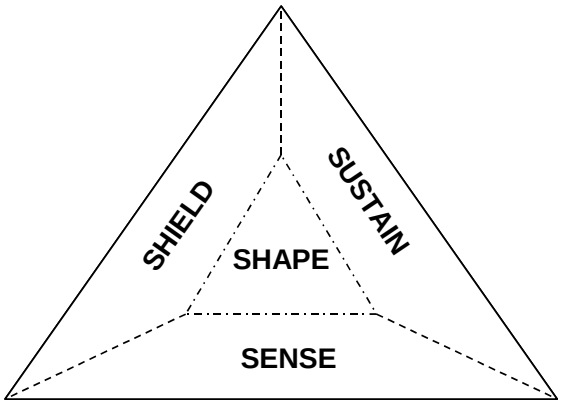

Figure B-2. CBRN Defense Joint Enabling Concepts
(a.k.a., the "4-S's" of CBRN Defense)

a. "SENSE" is the capability to continually provide information about the Chemical, Biological, Radiological and Nuclear (CBRN) situation at a time and place by detecting, identifying, and quantifying CBRN hazards in air, water, on land, on personnel, equipment or facilities. This capability includes detecting, identifying, and quantifying those CBRN hazards in all physical states (solid, liquid, gas). "Sense" is the key enabler to help emergency responders assess and understand CBRN hazards.

(1) "Sense" procedures should detect and identify immediate CBRN hazards in the air; on mission-critical work areas and equipment; on personnel; in water, food, or soil; on equipment or facilities.

(2) "Sense" procedures should determine the extent of the hazard (based on available sensing equipment), support protection and mission planning decisions, and confirm operationally significant hazards have been removed, reduced or eliminated.

(3) Use sensors to monitor and warn of the presence of CBRN hazards at key points or critical missions on an installation, particularly during increased threat conditions. Selective CBRN sensor use, though, may be smarter than continuous around-the-clock monitoring.

b. "SHAPE" provides the ability to characterize the CBRN hazard for the force commander. "Shape" supports command decisions to protect personnel and continue critical missions.

(1) Develop a clear understanding of the current and predicted CBRN situation.

(2) Collect, query, and assimilate information from sensors, intelligence, medical, etc., in near real time.

(3) Inform personnel as appropriate of CBRN hazards.

(4) Provide actual and potential impacts of CBRN hazards.

(5) Envision critical SENSE, SHIELD and SUSTAIN end states (preparation for operations).

(6) Visualize the sequence of events that moves the force from its current state to those end states.

c. "SHIELD" protects the force from harm caused by CBRN hazards by preventing or reducing individual and collective exposures, applying prophylaxis to prevent or mitigate negative physiological effects, and protecting critical equipment. The installation commander:

(1) Prevents or reduces CBRN casualties by reducing the threat, reducing operational vulnerability, and avoiding exposure.

(2) Provides appropriate levels of physical protection, medical treatment, or evacuation procedures to minimize casualties as possible (given equipment and treatment available).

(3) Must prepare to continue critical missions while minimizing potential CBRN hazard exposure.

(4) Relies on emergency responders through rapid response, assessment, and initial recovery operations. *[See reference (u)].*

(5) Takes steps to safeguard personnel from continued hazards, to control contamination, and to initiate steps to restore the area to its pre-incident conditions.

(6) Must coordinate with local, state, and regional emergency agencies to coordinate mutual assistance.

d. "SUSTAIN" includes actions to continue critical missions, respond appropriately, protect personnel, and restore combat power after a CBRN incident. Decontamination and medical actions, for example, enable an installation to facilitate a return to pre-incident operational capability as soon as possible.

(1) Depending on the operational impact of a CBRN incident, installation recovery efforts might be delayed in order to restore critical missions

or essential operations.

(2) Crime scene and epidemiological investigations may also be needed.

(3) Eventually the installation should be restored to pre-incident operation capability levels.

(4) Emergency response, thorough decontamination, long-term remediation and recovery, and mortuary affairs must be coordinated with local, state, federal (or host nation) emergency response agencies. Installation commanders should integrate capabilities from external agencies in order to sustain continuous capabilities.

(5) Installation commanders must be prepared to transition from emergency response to federal incident control and then back to DOD control during long-term restoration and recovery. Transitions must be done together with local, state, federal, host nation, and Service assets used in a military-civilian partnership.

AT Attributes	**AT Abilities**	**CBRN Joint Enabling Concepts**
Detect	The location, nature and intent of hostile efforts	Sense and Shape
Assess	Adversarial courses of action	Sense and Shape
Warn	The joint force in a timely, accurate and unambiguous manner	Shape and Shield
Prevent/ deter	The enemy from creating adverse effects	Shape and Shield
Defend	Personnel, physical assets, and information from adverse effects	Sense, Shape, Shield & Sustain
Recover	Without critical losses in operational effectiveness	Shape, Shield, & Sustain

Table B-2. CBRN Equivalent Concepts to DOD AT Attributes

[Source for AT Attributes and Abilities: Reference (k)]

5. Table B-2 (above) shows the CBRN Joint Enabling Concepts are similar to the existing AT Attributes, but do not correlate directly.

a. Some CBRN attributes (e.g., standoff detection) may not be technologically available or affordable for installations in the near term.

b. The CBRN Joint Enabling Concepts should be implemented through the judicious application of existing manpower and adapting current tactics, techniques, and procedures (TTPs).

ENCLOSURE C

References

a. United States Code, Title 14, Part 1, Chapter 1, (14 USC 1)

b. 50 US Code 1522, Conduct of the Chemical and Biological Defense Program, National Defense Authorization Act for Fiscal Year 1994

c. "Federal Response Plan (FRP) - Interim," Federal Emergency Management Agency (FEMA) 9230.1-PL, Terrorism Incident Annex

d. "Federal Radiological Emergency Response Plan (FRERP)," Federal Emergency Management Agency (FEMA), May 8, 1996,

e. "Initial National Response Plan," U.S. Department of Homeland Security, September 30, 2003.

f. "National Incident Management System (NIMS)," U.S. Department of Homeland Security, March 1, 2004.

g. Homeland Security Presidential Security Directive/HSPD-5, February 28, 2003, "Management of Domestic Incidents."

h. Homeland Security Presidential Security Directive/HSPD-7, December 17, 2003, "Critical Infrastructure Identification, Prioritization, and Protection."

i. Homeland Security Presidential Security Directive/HSPD-8, December 17, 2003, "National Preparedness."

j. U.S. Dept. of Homeland Security (DHS), September 30, 2003, "Initial National Response Plan."

k. "DOD CONOPS for Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive (CBRNE) Defense of U.S. Military Installations and Facilities Worldwide."

l. Under Secretary of Defense Acquisition Technology and Logistics Memorandum, 22 April 2003, Subject: Implementation Plan for Management of the Chemical and Biological Defense Program (CBDP)

m. DepSecDef Memorandum, September 5, 2002, "Preparedness of U.S. Military Installations and Facilities Worldwide Against Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive (CBRNE) Attack"

n. DepSecDef Memorandum, January 26, 2004, "Initial National Response Plan"

o. DOD Directive 2000.12, "DOD Antiterrorism (AT) Program"

p. DOD Directive 3025.1, "Military Support to Civil Authorities (MSCA)"

q. DOD Directive 3025.15, "Military Assistance to Civil Authorities (MACA)"

r. DOD Directive 5111.1, Under Secretary of Defense for Policy (USD(P))

s. DOD Directive 5134.8, Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense Programs (ATSD(NCB))

t. DOD Instruction 2000.16, "DOD Antiterrorism Standards"

u. DOD Instruction 2000.18, "DOD Installation Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive Emergency Response Guidelines"

v. DOD Instruction 5210.84, "Security of DOD Personnel at U.S. Missions Abroad"

w. DOD O-2000.12H, "DOD Antiterrorism Handbook, February 2004"

x. "DOD Critical Infrastructure Protection (CIP) Plan," 18 Nov 1998

y. "DOD Protection Joint Functional Concept," 31 Dec 2003

z. 2002 Unified Command Plan

aa. Unified Facilities Criteria 4-010-01, "DOD Minimum AT Standards for Buildings"

bb. Unified Facilities Criteria 4-010-10, "DOD Minimum Antiterrorism Standoff Distances for Buildings"

GLOSSARY

PART I – ABBREVIATIONS AND ACRONYMS

AOR	Area of Responsibility
ATSD(NCB)	Assistant to the Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs
ASD(HD)	Assistant Secretary of Defense for Homeland Defense
AT	Antiterrorism
BSA	Balanced Survivability Assessment
CBRN	Chemical, biological, radiological, and nuclear
CBRNE	Chemical, Biological, Radiological, Nuclear, and high-yield Explosive
CIP	Critical Infrastructure Protection
CJCS	Chairman of the Joint Chiefs of Staff
CM	Consequence Management
COCOM	Combatant Commander
CONUS	Continental United States
COOP	Continuity of Operations
COTS	Commercial-Off-The-Shelf
DOD	Department of Defense
FCM	Foreign consequence management
FP	Force protection
FPCON	Force protection condition
FRERP	Federal Radiological Emergency Response Plan
FRP	Federal Response Plan
GOTS	Government-Off-The-Shelf
JP	Joint Publication
JULLS	Joint Universal Lessons Learned System
JPEO-CBD	Joint Program Executive Office for Chemical-Biological Defense
JRO-CBRN Defense	J-8 Joint Requirements Office for Chemical, Biological, Radiological, and Nuclear Defense
JSIPP	Joint Services Installation Pilot Project
JSIVA	Joint Staff Installation Vulnerability Assessment
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MSCA	Military Support to Civil Authorities

NIOSH	National Institute for Occupational Safety and Health
NIMS	National Incident Management System
NRP	National Response Plan
OCONUS	Outside Continental United States
OSHA	Occupational Safety and Health Administration
POD	Port of Debarkation
POE	Port of Embarkation
PSA	Principal Staff Assistant
SECDEF	Secretary of Defense
SME	Subject Matter Expert
SOFA	Status of Forces Agreement
USC	United States Code
USG	United States Government
WMD	Weapons of Mass Destruction

PART II – DEFINITIONS

Antiterrorism (AT) - Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces. (JP 1-02; JP 3-07.2)

Base - 1. A locality from which operations are projected or supported. 2. An area or locality containing installations which provide logistic or other support. 3. (DOD only) Home airfield or home carrier. (JP 1-02)

Casualty - Any person who is lost to the organization by having been declared dead, duty status – whereabouts unknown, missing, ill, or injured. (JP 1-02)

CBRN Defense - Efforts to protect personnel on military installations and facilities from chemical, biological, radiological, and nuclear (CBRN) incidents. *[Note: Does not include defense from high-yield explosives.]*

CBRNE Hazards - Those toxic chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) hazards that are released in the presence of US forces or civilians. CBRNE hazards include those created from accidental releases, toxic industrial chemicals (especially air and water poisons), biological pathogens, radioactive matter, and high-yield explosives. Also included are any hazards resulting from the deliberate employment of weapons of mass destruction during military operations.

CBRNE Protection - Efforts to protect personnel and infrastructure on military installations and facilities from chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) incidents. Note: Includes defensive efforts from high-yield explosives.

Combatant Command (COCOM) - Nontransferable command authority established by title 10 ("Armed Forces"), United States Code, section 164, exercised only by commanders of unified or specified combatant commands unless otherwise directed by the President or the Secretary of Defense. Combatant command (command authority) cannot be delegated and is the authority of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command. Combatant command (command authority) should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and Service and/or functional component commanders. Combatant command (command authority) provides full authority to organize and employ commands and forces as the combatant commander considers necessary to accomplish assigned missions. Operational control is inherent in combatant command (command authority). (JP 1-02)

Combatant Commander - A commander of one of the unified or specified combatant commands established by the President. (JP 1-02)

Components – (This instruction only) The Military Departments (i.e., "Services") and the Chairman of the Joint Chiefs of Staff (CJCS). Other DOD entities, (i.e., Combatant Commands, DOD Agencies, DOD Field Activities, the Office of the Secretary of Defense, the Office of the Inspector General of the Department of Defense) may elect to follow this guidance as well.

Consequence Management (CM) –

(1) Those measures taken to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of a chemical, biological, nuclear, and/or high-yield explosive situation. For domestic consequence management, the primary authority rests with the States to respond and the Federal Government to provide assistance as required. [For the purposes of this Instruction, "nuclear" includes "radiological."] (JP 1-02; JP 3-0)

(2) Measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of terrorism.

(Federal Response Plan - Interim, Terrorism Incident Annex *[See reference (c)]*).

(3) *Note: This term is projected to be merged with "crisis management" to become "incident management" in accordance with the anticipated National Response Plan.*

Contamination –

(1) The deposit, absorption, or adsorption of radioactive material, or of biological or chemical agents on or by structures, areas, personnel, or objects. (JP 1-02)

(2) (DOD only) Food and/or water made unfit for consumption by humans or animals because of the presence of environmental chemicals, radioactive elements, bacteria or organisms, the byproduct of the growth of bacteria or organisms, the decomposing material (to include the food substance itself), or waste in the food or water. (JP 1-02)

Contamination Control - Procedures to avoid, reduce, remove, or render harmless (temporarily or permanently) nuclear, biological, and chemical contamination for the purpose of maintaining or enhancing the efficient conduct of military operations. (JP 1-02; JP 3-11)

Crisis - An incident or situation involving a threat to the United States, its territories, citizens, military forces, possessions, or vital interests that develops rapidly and creates a condition of such diplomatic, economic, political, or military importance that commitment of US military forces and resources is contemplated in order to achieve national objectives. (JP 1-02; JP 5-0)

Crisis Management. –

(1) Measures to resolve a hostile situation and investigate and prepare a criminal case for prosecution under federal law. Crisis management will include a response to an incident involving a weapon of mass destruction, special improvised explosive device, or a hostage crisis that is beyond the capability of the lead federal agency. (JP 1-02; JP 3-07.6)

(2) Measures to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or act of terrorism. (Federal Response Plan - Interim, Terrorism Incident Annex *[See reference (c)]).*

(3) *Note: This term is projected to be merged with "consequence management" to become "incident management" in accordance with the anticipated National Response Plan.*

Critical Asset — (DOD) A specific entity that is of such extraordinary importance to DOD operations in peace, crisis, and war that it its incapacitation or destruction would have a very serious, debilitating effect on the operation of the infrastructure which it supports to fulfill a DOD mission capability that is essential for DOD to execute the National Military Strategy.

Critical Infrastructure: That infrastructure, made functional by supporting critical assets, which, when any (or all) of those critical assets are incapacitated or destroyed, result in that infrastructure being unable to fulfill its functional purpose.

Critical Infrastructure Protection (CIP) –

(1) Department of Defense (DOD) program to identify and protect assets critical to the Defense Transportation System. Loss of a critical asset would result in failure to support the mission of a combatant commander. Assets include worldwide DOD, commercial, and civil physical and command, control, communications, computers, and intelligence infrastructures. (JP 1-02; JP 4-01)

(2) The identification, assessment, and security enhancement of physical and cyber assets and associated infrastructures essential to the execution of the National Military Strategy. CIP is a complementary program linking the protection aspects of Antiterrorism, Force Protection, Information Assurance, Continuity of Operations, and Readiness programs.

Criticality Assessment - Identifies key assets and infrastructure that support DOD missions, units, or activities and are deemed mission critical by military commanders or civilian agency managers. It addresses the impact of temporary or permanent loss of key assets or infrastructures to the installation or a unit's ability to perform its mission. It examines costs of recovery and reconstitution including time, dollars, capability, and infrastructure support. (DODD 2000.12)

Critical Military Missions - Any mission deemed critical to the successful completion of DOD operations in peace, crisis and war (as outlined in the National Military Strategy) must continue operating and be protected from disruption, degradation, and destruction plus be restored quickly if damaged. Facilities, equipment, and personnel essential to continue those critical missions shall receive second highest priority for protection behind emergency responders.

Critical Node - An element, position, or command and control entity whose disruption or destruction immediately degrades the ability of a force to command, control, or effectively conduct combat operations. (JP 1-02)

Critical Personnel. Personnel deemed essential to the performance of critical military missions (whether military, civilian, contractor, host nation personnel or third country nationals).

Defense Critical Infrastructure (DCI): That critical infrastructure inherent to the national critical infrastructure considered essential for DOD to execute the national military strategy. The infrastructure can be DOD owned or operated, exist in the commercial or other government sectors, or be located outside the United States. Defense infrastructure sectors include: Personnel; financial services; intelligence surveillance and reconnaissance (ISR); logistics; transportation; public works; global information grid (GIG); command control and communications; space; health affairs; and the defense industrial base (DIB).

DOD civilian - A Federal civilian employee of the Department of Defense directly hired and paid from appropriated or nonappropriated funds, under permanent or temporary appointment. Specifically excluded are contractors and foreign host nationals as well as third country civilians. (JP 1-03.17)

Emergency-Essential Employee - A Department of Defense civilian employee whose assigned duties and responsibilities must be accomplished following the evacuation of non-essential personnel (including dependents) during a declared emergency or outbreak of war. The position occupied cannot be converted to a military billet because it requires uninterrupted performance so as to provide immediate and continuing support for combat operations and/or combat systems support functions. (JP 1-02)

Emergency Responders - Personnel who work closest to known or suspected CBRNE hazards (e.g., security, fire, medical, CBRNE specialists).

Essential Military Operations - Operations deemed less than critical but still essential to the successful completion of DOD operations in peace, crisis and war. Essential functions must be reasonably protected from disruption, degradation, and destruction plus be restored quickly if damaged. Facilities, equipment, and personnel necessary to continue essential operations shall receive the third highest priority for protection (i.e., behind emergency responders and personnel assigned to critical missions).

Essential Personnel - Personnel deemed essential to the performance of essential military operations (whether military, civilian, contractor, host nation personnel or third country nationals).

Explosive Ordnance - All munitions containing explosives, nuclear fission or fusion materials, and biological and chemical agents. This includes bombs and warheads; guided and ballistic missiles; artillery, mortar, rocket, and small arms ammunition; all mines, torpedoes, and depth charges; demolition charges; pyrotechnics; clusters and dispensers; cartridge and propellant actuated devices; electro-explosive devices; clandestine and improvised explosive devices; and all similar or related items or components explosive in nature. (JP 1-02)

Explosive Ordnance Disposal (EOD) — The detection, identification, on-site evaluation, rendering safe, recovery, and final disposal of unexploded explosive ordnance. It may also include explosive ordnance which has become hazardous by damage or deterioration. (JP 1-02)

Explosive Ordnance Disposal Incident — The suspected or detected presence of unexploded or damaged explosive ordnance which constitutes a hazard to operations, installations, personnel, or material. Not included in this definition are the accidental arming or other conditions that develop during the manufacture of high explosive material, technical service assembly operations or the laying of mines and demolition charges. (JP 1-02)

Facility - A real property entity consisting of one or more of the following: a building, a structure, a utility system, pavement, and underlying land. (JP 1-02)

Force - An aggregation of military personnel, weapon systems, equipment, and necessary support, or combination thereof. (JP 1-02)

Force protection (FP) -

(1) [JP 1-02] Actions taken to prevent or mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information. These actions conserve the force's fighting potential so it can be applied at the decisive time and place and incorporate the coordinated and synchronized offensive and defensive measures to enable the effective employment of the joint force while degrading opportunities for the enemy. Force protection does not include actions to defeat the enemy or protect against accidents, weather or disease. (JP 3-0)

(2) [DODD 2000.12] Actions taken to prevent or mitigate hostile actions against DOD personnel (including family members), resources, facilities, and critical information. These actions conserve the force's fighting potential so it can be applied at the decisive time and place and incorporate the coordinated and synchronized offensive and defensive measures to enable the effective employment of the Joint Force while

degrading the opportunities of the enemy. Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease.

Force Protection Condition (FPCON) -

(1) [JP1-02, except FPCON NORMAL] A Chairman of the Joint Chiefs of Staff-approved program standardizing the Military Services' identification of and recommended responses to terrorist threats against US personnel and facilities. This program facilitates inter-Service coordination and support for antiterrorism activities. There are four FPCONs above normal.

a. FPCON NORMAL - A general threat of possible terrorist activity exists, but warrants a routine security posture.

b. FPCON ALPHA - This condition applies when there is a general threat of possible terrorist activity against personnel and facilities, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of FPCON BRAVO measures. However, it may be necessary to implement certain measures from higher FPCONs resulting from intelligence received or as a deterrent. The measures in this FPCON must be capable of being maintained indefinitely.

c. FPCON BRAVO - This condition applies when an increased and more predictable threat of terrorist activity exists. The measures in this FPCON must be capable of being maintained for weeks without causing undue hardship, affecting operational capability, and aggravating relations with local authorities.

d. FPCON CHARLIE - This condition applies when an incident occurs or intelligence is received indicating some form of terrorist action against personnel and facilities is imminent. Implementation of measures in this FPCON for more than a short period probably will create hardship and affect the peacetime activities of the unit and its personnel.

e. FPCON DELTA — This condition applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is likely. Normally, this FPCON is declared as a localized condition.

(2) (DODD 2000.12) A DOD-approved and mandated system standardizing the Department's identification, recommended protective actions, and responses to terrorist threats against U.S. personnel and facilities. This system is the principal means for a commander to apply an operational

decision on how to protect against terrorism and facilitates inter-Service coordination and support for antiterrorism activities.

Foreign Consequence Management (FCM) - Those efforts that comprise interagency assistance overseas to respond and mitigate damage occurring from a CBRNE incident. Foreign CM response may require specialized hazard material handling, decontamination, urban search and rescue and medical efforts in addition to traditional foreign disaster relief efforts. (CJCSI 3214.01A) *Note: Department of State is lead federal agency for FCM.*

Hardened Site - A site, normally constructed under rock or concrete cover, designed to provide protection against the effects of conventional weapons. It may also be equipped to provide protection against the side effects of a nuclear attack and against a chemical or a biological attack. (JP 1-02)

Host Nation (HN) - A nation that receives the forces and/or supplies of allied nations, coalition partners, and/or NATO organizations to be located on, to operate in, or to transit through its territory. (JP 1-02)

Host-Nation Support Agreement - Basic agreement normally concluded at government-to-government or government-to-combatant commander level. These agreements may include general agreements, umbrella agreements, and memoranda of understanding. (JP 4-01.8)

Infrastructure –

(1) All building and permanent installations necessary for the support, redeployment, and military forces operations (e.g., barracks, headquarters, airfields, communications, facilities, stores, port installations, and maintenance stations). (JP 1-02, JP 4-01.8)

(2) The framework of interdependent physical and cyber-based systems, made functional by supporting assets, which comprise identifiable industries, institutions, networks, and distribution capabilities that enable a continued flow of goods and services required for the defense and economic security of the United States, the smooth functioning of Government at all levels, and society. (Draft DODD 3020)

Installation - A grouping of facilities, located in the same vicinity, which support particular functions. Installations may be elements of a base. (JP 1-02)

Installation Commander - The individual responsible for all operations performed by an installation. (JP 3-07.2)

Installation Protection – An aggregation of installation functions with a similar broad goal to continue critical DOD missions, respond appropriately to CBRNE incidents, protect personnel, and restore essential operations expeditiously following a CBRNE incident. Incident management for installation protection includes all functions that prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies.

Integration - 1. In force protection, the synchronized transfer of units into an operational commander's force prior to mission execution. 2. The arrangement of military forces and their actions to create a force that operates by engaging as a whole. (JP 0-2)

Joint Base - For purposes of base defense operations, a joint base is a locality from which operations of two or more of the Military Departments are projected or supported and which is manned by significant elements of two or more Military Departments or in which significant elements of two or more Military Departments are located. (JP 3-10)

Key Facilities List - A register of selected command installations and industrial facilities of primary importance to the support of military operations or military production programs. It is prepared under the policy direction of the Joint Chiefs of Staff. (JP 1-02)

Lessons Learned - Actionable item resulting in appropriate change to policy, guidance, or procedures. Such items are typically derived from observations and concerns acquired through experience, exercises, or after-action reviews.

Local Authorities - Any county, city, village, town, district, or other political subdivision of a state, any Native American tribe or authorized tribal organization, or Alaska native village or organization, and includes any rural community or unincorporated town or village or any other public entity for which an application for assistance is made by a state or political subdivision thereof. (National Strategy for Homeland Defense)

Mass Casualty - Any large number of casualties produced in a relatively short period of time, usually as the result of a single incident such as a military aircraft accident, hurricane, flood, earthquake, or armed attack that exceeds local logistic support capabilities. (JP 1-02)

Military Installation - A base, camp, post, station, yard, center, or other activity under the jurisdiction of the Secretary of a Military Department or, in the case of an activity in a foreign country, under the operational control of the Secretary of a Military Department or the Secretary of Defense. (JP 4-04)

Mission-Essential Functions – Those continuing functions that must be performed to achieve the DOD's critical missions. Those comprise, but are not

limited to, the following: (a) command and control of assets, (b) the receipt, assessment, analysis, processing, display, and dissemination of information necessary to perform critical missions and support decision making, and (c) other operations that must be performed to achieve mission success. (DODD 3020.26)

National Critical Infrastructure (NCI): That critical infrastructure considered essential to the functioning of the nation and whose capacity or destruction would have a debilitating regional or national impact. It includes but is not limited to telecommunications, electrical power systems, gas and oil transportation and storage, water supply systems, banking and finance, transportation emergency services, industrial complexes, information systems, and continuity of government operations. (Draft DODD 3020)

Other People – All people on an installation who are not considered emergency responders, critical personnel, or essential personnel. Most dependents, for example, would likely be in this category.

Overseas (OCONUS) - All locations, including Alaska and Hawaii, outside the continental United States. (JP 1-02)

Personnel - Those individuals required in either a military or civilian capacity to accomplish the assigned mission. (JP 1-02)

Port of Debarkation (POD) - The geographic point at which cargo or personnel are discharged. This may be a seaport or aerial port of debarkation; for unit requirements; it may or may not coincide with the destination. (JP 1-02)

Port of Embarkation (POE) - The geographic point in a routing scheme from which cargo or personnel depart. This may be a seaport or aerial port from which personnel and equipment flow to a port of debarkation; for unit and non-unit requirements, it may or may not coincide with the origin. (JP 1-02)

Protection - Measures that are taken to keep nuclear, biological, and chemical hazards from having an adverse effect on personnel, equipment, or critical assets and facilities. Protection consists of five groups of activities: hardening of positions; protecting personnel; assuming mission-oriented protective posture; using physical defense measures; and reacting to attack. (JP 3-14)

Protect Personnel - Evacuate or protect personnel (as appropriate) in the hazard area (including downwind) that are not involved in CBRNE incident response or continuing critical missions.

Respond Appropriately - Respond appropriately with emergency responders to mitigate the impact of CBRNE incidents. As personnel closest to CBRNE hazards, emergency responders receive the highest level of protection. CBRNE

incident response must balance the needs to assess the situation, secure the area, find and suppress hazards (e.g., fires, UXOs, contamination), establish control, evacuate personnel as appropriate, handle casualties, and preserve evidence.

Restoration of Operations - Efforts to restore military and/or civil operations to pre-incident productivity levels (or better). These efforts are not as time-sensitive as restoring "critical military missions" or "essential military operations." Hazards from CBRNE contamination can be completely removed or neutralized (e.g., full environmental restoration) as resources allow.

Sea Port - A land facility designated for reception of personnel or materiel moved by sea, and that serves as an authorized port of entrance into or departure from the country in which located. (JP 1-02)

Sense - The capability to stay aware of the current CBRN situation by detecting and (if possible) identifying CBRN hazards: (a) in the air, water, food, or soil; (b) on personnel, equipment, or facilities; or (c) hazard state (i.e., solid, liquid, gaseous).

Services - Refers to the Army, Navy, Air Force, Marine Corps, and Coast Guard *[reference (a)].*

Shape. The capability to characterize the CBRN hazard for the installation commander. CBRN characterization is a process to help commanders understand the current and projected CBRN hazard situation so they can make appropriate and timely decisions to shield the force and sustain mission operations.

Shield - The capability to prevent or reduce casualties under CBRN hazard conditions by reducing the threat, reducing operational vulnerability, and avoiding contamination.

Standards - Implementation of "standardization," whereby DOD "achieves the closest practicable cooperation among the Services and Defense agencies for the most efficient use of research, development, and production resources, and agrees to adopt on the broadest possible basis the use of: a. common or compatible operational, administrative, and logistic procedures; b. common or compatible technical procedures and criteria; c. common, compatible, or interchangeable supplies, components, weapons, or equipment; and d. common or compatible tactical doctrine with corresponding organizational compatibility." (JP 1-02)

Sustain - The capability to continue critical operations during a CBRNE incident, resume essential operations quickly after a CBRNE incident, and fully

restore the installation over time. Actions to mitigate the severity of CBRNE incidents also may be included here.

Terrorism - The calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological. (JP 3-07.2)

Terrorist - An individual who uses violence, terror, and intimidation to achieve a result. (JP 3-07.2)

Terrorist Groups - Any element, regardless of size or espoused cause, that commits acts of violence or threatens violence in pursuit of its political, religious, or ideological objectives. (JP 3-07.2)

Terrorist Incident - A violent act, or an act dangerous to human life, in violation of the criminal laws of the United States or of any State, to intimidate or coerce a government, the civilian population, or any segment thereof in furtherance of political or social objectives. (FBI definition [as Lead Federal Agency], as shown in Federal Response Plan - Interim, Terrorist Incident Annex *[See reference (c)]).*

Terrorist Threat_Level - An intelligence threat assessment of the level of terrorist threat faced by US personnel and interests. The assessment is based on a continuous intelligence analysis of a minimum of four elements: terrorist group operational capability, intentions, activity, and operational environment. There are four threat levels: LOW, MODERATE, SIGNIFICANT, and HIGH. Threat levels should not be confused with force protection conditions (FPCON). Threat level assessments are provided to senior leaders to assist them in determining the appropriate local FPCON. (Department of State also makes threat assessments, which may differ from those determined by Department of Defense.) *(DODD 2000.12)*

Threat Analysis - In antiterrorism, a continual process of compiling and examining all available information concerning potential terrorist activities by terrorist groups which could target a facility. A threat analysis will review the factors of a terrorist group's existence, capability, intentions, history, and targeting, as well as the security environment within which friendly forces operate. Threat analysis is an essential step in identifying probability of terrorist attack and results in a threat assessment. (JP 3-07.2)

Threat and Vulnerability Assessment - In antiterrorism, the pairing of a facility's threat analysis and vulnerability analysis. (JP 3-07.2)

Threat Identification and Assessment - The Joint Operation Planning and Execution System function that provides: timely warning of potential threats to US interests; intelligence collection requirements; the effects of environmental,

physical, and health hazards, and cultural factors on friendly and enemy operations; and determines the enemy military posture and possible intentions. (JP 1-02)

Vulnerability. - 1. The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. 2. The characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment.
(JP 1-02)

Vulnerability Assessment (VA) - A Department of Defense, command, or unit-level evaluation (assessment) to determine the vulnerability of a terrorist attack against an installation, unit, exercise, port, ship, residence, facility, or other site. Identifies areas of improvement to withstand, mitigate, or deter acts of violence, or terrorism. (JP 1-02)

Weapons of Mass Destruction (WMD) -

(1) [JP 1-02] Weapons that are capable of a high order of destruction and/or of being used in such a manner as to destroy large numbers of people. Weapons of mass destruction can be high explosives or nuclear, biological, chemical, and radiological weapons, but exclude the means of transporting or propelling the weapon where such means is a separable and divisible part of the weapon.

(2) [Title 18, U.S.C. 2332a (FBI definition), as shown in Federal Response Plan - Interim, Terrorist Incident Annex *[See reference (c)]*.] (1) Any destructive device as defined in Section 921 of this title, [which reads] any explosive, incendiary, or poison gas, bomb, grenade, rocket having a propellant charge of more than four ounces, missile having an explosive or incendiary charge of more than one-quarter ounce, mine, or device similar to the above; (2) poison gas; (3) any weapon involving a disease organism; or (4) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life.